

**Notice of Allowability**

Application No.

09/596,663

Examiner

Abdulahkim Nobahar

Applicant(s)

GAVAGNI ET AL.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 31 May 2005.
2. ☒ The allowed claim(s) is/are 1-40.
3. ☒ The drawings filed on 19 June 2000 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All   b) ☐ Some\*   c) ☐ None   of the:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  6. ☐ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
    - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
      - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
    - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- |   |  |
|---|--|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892)  | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)            |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                | 6. <input type="checkbox"/> Interview Summary (PTO-413),<br>Paper No./Mail Date _____. |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),<br>Paper No./Mail Date _____ | 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment                    |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit<br>of Biological Material          | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance   |
|   | 9. <input type="checkbox"/> Other _____.   |

PD

## **DETAILED ACTION**

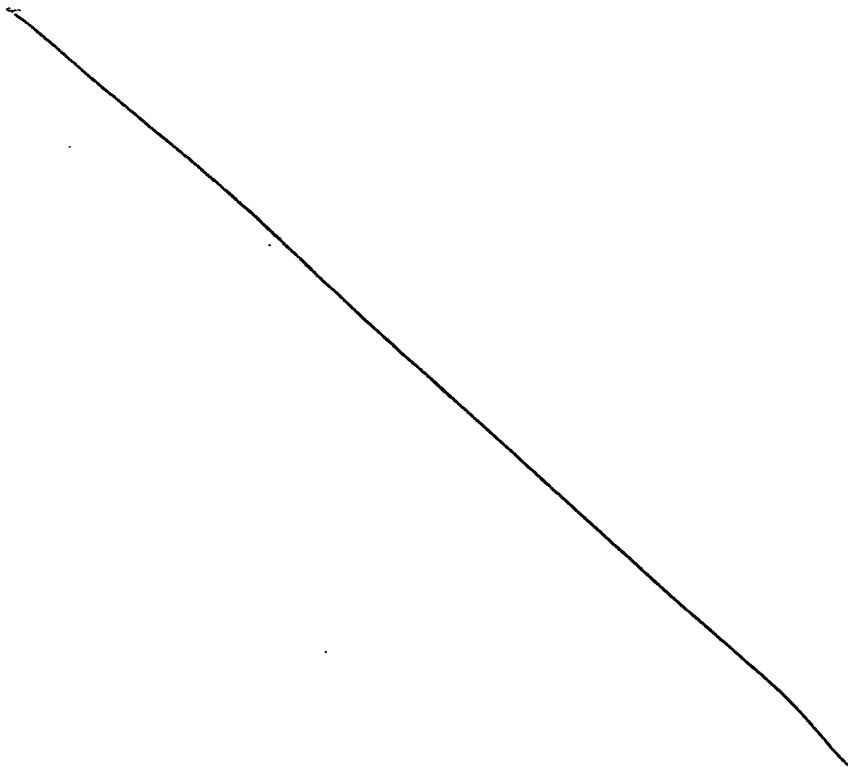
### **EXAMINER'S AMENDMENT**

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Gregory A. Nelson on June 20, 2005.

The application has been amended as follows:

Please enter the following readable copy of amendments to claims as replacement to the amended claims file on May 31, 2005:



Appln. No. 09/596,663  
RCE dated May 31, 2005  
Reply to Advisory Action of April 29, 2005  
Docket No. 6169-159

IBM Docket No. BOC9-2000-0014

Page 3

**Amendments to Claims:**

This listing of claims will replace all prior versions and listings of claims in the instant application:

**Listing of Claims:**

1. (Currently Amended) A method for performing secured communications between a Voice Browser and a network device, said Voice Browser and network device exchanging VoiceXML-based Web content comprising the steps of:
  - a Voice Browser receiving an audible request from a user, said audible request being a request for Web content;
  - responsive to said audible request, the Voice Browser transmitting a request to the network device associated with the Web-based content to establish a secured communication session between the Voice Browser and the network device;
  - authenticating the network device;
  - subsequent to said authentication, negotiating a shared secret between the network device and the Voice Browser;
  - encrypting the VoiceXML-based Web content using said shared secret as an encryption key;
  - exchanging the encrypted VoiceXML-based Web content between the network device and the Voice Browser; [[and,]]
  - decrypting the VoiceXML-based Web content using said shared secret as a decryption key[[.]] ; and
  - the Voice Browser audibly presenting the decrypted Web content to said user.

~~Appln. No. 09/596,663  
RCE dated May 31, 2005  
Reply to Advisory Action of April 29, 2005  
Docket No. 6169-159~~

~~IBM Docket No. BOC9-2006-0014~~

~~Page 4~~

2. (Original) The method of claim 1, wherein said step of authenticating the network device comprises the steps of:  
transmitting a digital certificate from the network device to the Voice Browser, said digital certificate having a public key and a reference to a certificate authority; and,  
validating said certificate authority.
3. (Original) The method of claim 2, wherein said digital certificate is an X.509-compliant digital certificate.
4. (Original) The method of claim 1, further comprising the step of authenticating the Voice Browser.
5. (Original) The method of claim 4, wherein said step of authenticating the Voice Browser comprises the steps of:  
transmitting a digital certificate from the Voice Browser to the network device, said digital certificate having a public key and a reference to a certificate authority; and,  
validating said certificate authority.
6. (Original) The method of claim 5, wherein said digital certificate is an X.509-compliant digital certificate.
7. (Original) The method of claim 2, wherein said step of authenticating the network device further comprises the step of challenging the network device.

Appln. No. 09/596,663  
RCE dated May 31, 2005  
Reply to Advisory Action of April 29, 2005  
Docket No. 6169-159

IBM Docket No. BOC9-2000-0014

Page 5

8. (Original) The method of claim 5, wherein said step of authenticating the Voice Browser further comprises the step of challenging the Voice Browser.

9. (Original) The method of claim 7, wherein said step of challenging the network device comprises the steps of:

encrypting a message using said public key contained in said digital certificate;

transmitting said encrypted message from the Voice Browser to the network device;

decrypting said encrypted message using a private key corresponding to said public key; and,

transmitting the decrypted message to the Voice Browser.

10. (Original) The method of claim 8, wherein said step of challenging the Voice Browser comprises the steps of:

encrypting a message using said public key contained in said digital certificate;

transmitting said encrypted message from the network device to the Voice Browser;

decrypting said encrypted message using a private key corresponding to said public key; and,

transmitting the decrypted message to the network device.

11. (Original) The method of claim 1, wherein said negotiating step comprises the steps of:

generating a key for use in a symmetric cryptographic algorithm;

encrypting said generated key with said public key;

Appln. No. 09/596,663

RCE dated May 31, 2005

Reply to Advisory Action of April 29, 2005

Docket No. 6169-159

IBM Docket No. BOC9-2000-0014

Page 6

transmitting said encrypted key to the network device; and,  
decrypting said key in the network device with a private key corresponding to  
said public key.

12. (Original) The method of claim 1, wherein said negotiating step comprises  
the steps of:

generating a key for use in a symmetric cryptographic algorithm;  
encrypting said generated key with said public key;  
transmitting said encrypted key to the Voice Browser; and,  
decrypting said key in the Voice Browser with a private key corresponding to  
said public key.

13. (Original) The method of claim 1, further comprising the steps of:  
exchanging a list of supported symmetrical cryptographic algorithms for the  
network device and the Voice Browser;

selecting a symmetrical cryptographic algorithm from said list; and,  
performing said encrypting and decrypting steps using said selected  
symmetrical cryptographic algorithm.

14. (Original) The method of claim 1, wherein said Voice Browser is a  
VoiceXML Browser Server.

15. (Currently Amended) A method for performing secured communications  
in a Voice Browser comprising the steps of:

a Voice Browser receiving an audible request from a user, said audible request  
being a request for Web content;

Appln. No. 09/596,663  
RCE dated May 31, 2005  
Reply to Advisory Action of April 29, 2005  
Docket No. 6169-159

IBM Docket No. BOC9-2000-0014

Page 7

responsive to said audible request, the Voice Browser transmitting a request from the Voice Browser to a network device associated with the Web-based content for a secure communications session between the Voice Browser and the network device;

receiving from the network device a digital certificate containing a public key and a reference to a certificate authority.

authenticating the network device based on the digital certificate;

subsequent to said authentication, negotiating a shared secret with the network device;

encrypting data using said shared secret as an encryption key and transmitting said encrypted data to the network device;[[ and,]]

receiving encrypted Web content from the network device and decrypting the Web content using said shared secret as a decryption key; and,[[.]]

the Voice Browser audibly presenting the decrypted Web content to said user.

16. (Original) The method of claim 15, wherein said transmitting step further comprises the step of:

transmitting to said network device a list of supported encryption algorithms for use in said encryption and decryption steps,

said network device selecting an encryption algorithm from among said list.

17. (Original) The method of claim 16, wherein said data is encrypted using said selected encryption algorithm and said Web content is decrypted using said encryption algorithm.

18. (Original) The method of claim 15, wherein said digital certificate is an X.509-compliant digital certificate.

Appln. No. 09/596,663  
RCE dated May 31, 2005  
Reply to Advisory Action of April 29, 2005  
Docket No. 6169-159

IBM Docket No. BOC9-2000-0014

Page 8

19. (Original) The method of claim 15, wherein said Web content is a VoiceXML document.

20. (Original) The method of claim 19, wherein said Voice Browser is a VoiceXML Browser Server.

21. (Currently Amended) A machine readable storage, having stored thereon a computer program for performing secured communications between a Voice Browser and a network device, said Voice Browser and network device exchanging VoiceXML-based Web content, said computer program having a plurality of code sections executable by a machine for causing the machine to perform the steps of:

a voice browser receiving an audible request from a user, said audible request being a request for Web content;

responsive to said audible request, the Voice Browser transmitting a request to the network device associated with the Web-based content to establish a secured communication session between the Voice Browser and the network device;

authenticating the network device;

subsequent to said authentication, negotiating a shared secret between the network device and the Voice Browser;

encrypting the VoiceXML-based Web content using said shared secret as an encryption key;

exchanging the encrypted VoiceXML-based Web content between the network device and the Voice Browser; [[and,]]

decrypting the VoiceXML-based Web content using said shared secret as a decryption key[.]; and

the Voice Browser audibly presenting the decrypted Web content to said user.



Appln. No. 09/596,663  
RCE dated May 31, 2005  
Reply to Advisory Action of April 29, 2005  
Docket No. 6169-159

IBM Docket No. BOC9-2006-0014

page 9

22. (Original) The machine readable storage of claim 21, wherein said step of authenticating the network device comprises the steps of:

transmitting a digital certificate from the network device to the Voice Browser, said digital certificate having a public key and a reference to a certificate authority; and,

validating said certificate authority.

23. (Original) The machine readable storage of claim 22, wherein said digital certificate is an X.509-compliant digital certificate.

24. (Original) The machine readable storage of claim 21, for further causing the machine to perform the step of authenticating the Voice Browser.

25. (Original) The machine readable storage of claim 24, wherein said step of authenticating the Voice Browser comprises the steps of:

transmitting a digital certificate from the Voice Browser to the network device, said digital certificate having a public key and a reference to a certificate authority; and,

validating said certificate authority.

26. (Original) The machine readable storage of claim 25, wherein said digital certificate is an X.509-compliant digital certificate.

27. (Original) The machine readable storage of claim 22, wherein said step of authenticating the network device further comprises the step of challenging the network device.

Appl. No. 09/596,663  
RCE dated May 31, 2005  
Reply to Advisory Action of April 29, 2005  
Docket No. 6169-159

IBM Docket No. BOC9-2000-0014

page 10

28. (Original) The machine readable storage of claim 25, wherein said step of authenticating the Voice Browser further comprises the step of challenging the Voice Browser.

29. (Original) The machine readable storage of claim 27, wherein said step of challenging the network device comprises the steps of:

encrypting a message using said public key contained in said digital certificate;

transmitting said encrypted message from the Voice Browser to the network device;

decrypting said encrypted message using a private key corresponding to said public key; and,

transmitting the decrypted message to the Voice Browser.

30. (Original) The machine readable storage of claim 28, wherein said step of challenging the Voice Browser comprises the steps of:

encrypting a message using said public key contained in said digital certificate;

transmitting said encrypted message from the network device to the Voice Browser;

decrypting said encrypted message using a private key corresponding to said public key; and,

transmitting the decrypted message to the network device.

31. (Original) The machine readable storage of claim 21, wherein said negotiating step comprises the steps of:

Appln. No. 09/596,663  
RCE dated May 31, 2005  
Reply to Advisory Action of April 29, 2005  
Docket No. 6169-159

IBM Docket No. BOC9-2000-0014

Page 11

generating a key for use in a symmetric cryptographic algorithm;  
encrypting said generated key with said public key;  
transmitting said encrypted key to the network device; and,  
decrypting said key in the network device with a private key corresponding to  
said public key.

32. (Original) The machine readable storage of claim 21, wherein said  
negotiating step comprises the steps of:

generating a key for use in a symmetric cryptographic algorithm;  
encrypting said generated key with said public key;  
transmitting said encrypted key to the Voice Browser; and,  
decrypting said key in the Voice Browser with a private key corresponding to  
said public key.

33. (Original) The machine readable storage of claim 21, for further causing  
the machine to perform the steps of:

exchanging a list of supported symmetrical cryptographic algorithms for the  
network device and the Voice Browser;  
selecting a symmetrical cryptographic algorithm from said list; and,  
performing said encrypting and decrypting steps using said selected  
symmetrical cryptographic algorithm.

34. (Original) The machine readable storage of claim 21, wherein said Voice  
Browser is a VoiceXML Browser Server.

35. (Currently Amended) A machine readable storage, having stored thereon  
a computer program for performing secured communications in a Voice Browser,

Appln. No. 09/596,663  
RCE dated May 31, 2005  
Reply to Advisory Action of April 29, 2005  
Docket No. 6169-159

IBM Docket No. BOC9-2000-0614

Page 12

said computer program having a plurality of code sections executable by a machine for causing the machine to perform the steps of:

a Voice Browser receiving an audible request from a user, said audible request being a request for Web content;

responsive to said audible request, the Voice Browser transmitting a request from the Voice Browser to a network device associated with the Web-based content for a secure communications session between the Voice Browser and the network device;

receiving from the network device a digital certificate containing a public key and a reference to a certificate authority.

authenticating the network device based on the digital certificate;

subsequent to said authentication, negotiating a shared secret with the network device;

encrypting data using said shared secret as an encryption key and transmitting said encrypted data to the network device;[[ and,]]

receiving encrypted Web content from the network device and decrypting the Web content using said shared secret as a decryption key; and,[[.]]

the Voice Browser audibly presenting the decrypted Web content to said user.

36. (Original) The machine readable storage of claim 35, wherein said transmitting step further comprises the step of:

transmitting to said network device a list of supported encryption algorithms for use in said encryption and decryption steps,

said network device selecting an encryption algorithm from among said list.

Appl. No. 09/596,663  
RCE dated May 31, 2005  
Reply to Advisory Action of April 29, 2005  
Docket No. 6169-159

IBM Docket No. BOC9-2000-0014

page 13

37. (Original) The machine readable storage of claim 36, wherein said data is encrypted using said selected encryption algorithm and said Web content is decrypted using said encryption algorithm.

38. (Original) The machine readable storage of claim 35, wherein said digital certificate is an X.509-compliant digital certificate.

39. (Original) The machine readable storage of claim 35, wherein said Web content is a VoiceXML document.

40. (Original) The machine readable storage of claim 39, wherein said Voice Browser is a VoiceXML Browser Server.

***Allowable Subject Matter***

1. Claims 1-40 are allowed.
2. The following is an examiner's statement of reasons for allowance:
3. The primary reasons for the allowance of the independent claims 1, 15, 21 and 35 are the inclusion of the following limitation that is not found in the prior art and they are uniquely distinct features. The closest prior arts are Saylor et al (6,707,889 A1) and Jardin (6,681,327 B1). Saylor et al Saylor teaches a method for secure communication between a voice browser and a server with XML-based content transaction. Saylor also teaches an authentication process for a secure transaction between the Voice browser and the network server storing XML-based voice files. Jardin discloses a system for a secure client-server communication over Internet using a secure links such as secure socket layer (SSL) and IPSec. These two arts, singularly or in combination, fail to anticipate or render the following limitation:

"Claims 1, 15, 21 and 35: a Voice Browser receiving an audible request from a user, aid audible request being a request for Web content;

responsive to said audible request, the Voice Browser transmitting a request to the network device associated with the Web-based content to

Art Unit: 2132

establish a secured communication session between the Voice Browser and the network device; and

the Voice Browser audibly presenting the decrypted Web content to said user.”

4. The dependent claims 2-14, 16-20, 22-34 and 36-40 are allowed because they were originally found to include a unique feature not found in the closest abovementioned art.

### ***Conclusion***

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulahkim Nobahar  
Examiner  
Art Unit 2132

AN *a.n.*  
June 20, 2005

*Gilberto Barron Jr.*  
GILBERTO BARRON JR.  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100